

REMARKS

The applicant acknowledges and appreciates the Examiner's through examination of the application and request re-examination and reconsideration of the application in view of the preceding amendments and following remarks.

The Examiner objects to claim 1 due to an alleged informality. The applicants herein amend claim 1 as suggested by the Examiner and also amend to word "increase" to recite "inverse" to correct a typographical error. Accordingly, the applicants request that the Examiner withdraw the objection to claim 1.

Claims 1-31 stand rejected under 35 U.S.C. 101 because the claims allegedly are directed to non-statutory subject matter.

The Examiner alleges that claim 1 is directed to non-statutory subject matter since the subject invention provides a data encryption engine which may be implemented in software and/or hardware. However, the fact that an invention may be implemented in software does not preclude patentability under 35 USC 101. As described in section 2106 of the MPEP, "USPTO personnel must first identify whether the claim falls within at least one of the four enumerated categories of patentable subject matter recited in section 101 (i.e., process, machine, manufacture, or composition of matter)." (Emphasis added). Section 2106 of the MPEP also cites the well-known State Street decision to show the Federal Circuit has explained the same requirement:

The question of whether a claim encompasses statutory subject matter should not focus on which of the four categories of subject matter a claim is directed to -- process, machine, manufacture, or composition of matter -- [provided the subject matter falls into at least one category of statutory subject matter] but rather on the essential characteristics of the subject matter, in particular, its practical utility.

MPEP 2606 (emphasis added) (citing *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F3d 1368, 1373, 47 USPQ2d 1596, 1602 (Fed. Cir. 1998), cert. Dnd, 119 S. Ct. 851 (1999)). Thus, since the subject matter is clearly directed to an embodiment involving one of the four categories of statutory subject matter, e.g., a machine, it indeed is directed to statutory subject matter.

Moreover, since the subject invention is directed to statutory subject matter since it is directed to a practical application that produces a useful, concrete and tangible result. *See AT&T Corporation v. Excel Communications, Inc.*, 50 U.S.P.Q. 2d 1447, 1451 (Fed. Cir. 1999) (emphasis added) (citing *State Street Bank & Trust Co. v. Signature Financial Group*, 149 F3d 1368, 1373, 47 USPQ2d 1596, 1601 (Fed. Cir. 1998), cert. Dnd, 119 S. Ct. 851 (1999)). A specific useful, concrete and tangible result of the subject invention is that it provides a data encryption engine for implementing the advanced encryption standard (AES) for encryption or decryption. The subject invention as claimed by the applicants is used for the advanced encryption standard (AES) with real time S-box generation for generating in real time an advanced encryption standard cipher function of a first data block. See independent claim 1 and page 5, lines 2-3 of the subject application.

Thus, contrary to the Examiner's assertion, the advanced encryption standard (AES) engine of the subject invention clearly falls into one category of statutory subject matter and should be given patentable weight because it produces "a useful, concrete and tangible result." *Id.* Since the subject invention as claimed by the applicants recites statutory subject matter, applicants respectfully request that the Examiner withdraw this rejection to claims 1-31.

Claims 1, 12-15 and 29 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by US Patent Publication No. 2003/0039355 A1 to McCanny et al.

The invention results from the realization that an advanced encryption standard (AES) engine with real time S-box generation which is faster even than a parallel look-up approach can be achieved with the applicants' claimed Galois field multiplier system. In a first mode, the Galois field multiplier system is responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in $GF^{-1}(2^m)$ and applying an affine over $GF(2)$ transformation to obtain a subbyte transformation. A shift register system transforms the subbyte transformation to obtain a shift row transformation. In a second mode, the Galois field multiplier system is responsive to the shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of the first data block.

The operation in each mode and state may be performed by a separate Galois field linear transformer or a few or even just one Galois field linear transformer may be used and reconfigured by a programmer/controller to perform the different operations. The Galois field linear transformer may be compounded to perform more than one function in the operation.

McCanny et al. relates to a product for generating data encryption/decryption. Fig. 3 of McCanny et al. illustrates a round 24 of the Rijndael algorithm. Round 24 includes a ByteSub transformation 30, a ShiftRow transformation 32, a MixColumn transformation 34 and a Round Key Addition 36. *See* McCanny et al. at page 3, paragraph 41. Fig. 5 of McCanny et al. shows the corresponding modules, which includes ByteSub module 52, ShiftRow transformation module 54, MixColumn module 56 and Key Addition module 58. ByteSub module 52 uses 8

BlockSelect RAM (BRAM) storage devices for providing 16 look-up tables. MixColumn module 56 uses sixteen GF(28) 8-bit multiplier blocks 78.

The Examiner alleges in the Office Action that McCanny et al. discloses a Galois field multiplier system to obtain a subbyte transformation as claimed by the applicants. McCanny et al. clearly discloses, however, that it uses one or more look-up tables or ROMs to obtain a subbyte transformation and teaches away from the use of the applicants' claimed Galois field multiplier for the subbyte transformation:

A consideration in the design of the apparatus 40 is the memory requirement. The ByteSub module 52 is therefore advantageously implemented as one or more look-up tables (LUTs) or ROMs. This is a faster and more cost-effective (in terms of resources required) implementation than implementing the multiplicative inverse operation and affine transformation in logic.

McCanny et al. at page 4, paragraph 60 (emphasis added). Thus, McCanny et al. clearly teaches away from applicants' claimed advanced encryption standard (AES) engine with real time S-box generation that includes a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in $GF^1(2^m)$ and applying an affine over GF(2) transformation to obtain a subbyte transformation. Rather, McCanny et al. discloses and teaches that it is allegedly preferable to use one or more look-up tables (LUTs) or ROMs.

Moreover, McCanny et al. clearly fails to disclose a Galois field multiplier system as claimed by the applicants, specifically a Galois field multiplier system that obtains both the subbyte transformation in a first mode, and obtains a mix column transformation and adds a round key in a second mode. Rather, McCanny et al. clearly discloses using ByteSub module 52, which uses 8 BlockSelect RAM (BRAM) storage devices for providing sixteen look-up

tables as described above, a MixColumn module 56 which includes multiplier blocks 78 and a Key Addition module 58. McCanny et al. fails to disclose a Galois field multiplier system that operates in first and second modes as claimed by the applicants to perform these three operations.

In contrast to McCanny et al., the subject invention teaches that a Galois field multiplier system may be used to perform these three operations. The operation in each mode and state may be performed by a separate Galois field linear transformer or a few or even just one Galois field linear transformer may be used and reconfigured by a programmer/controller to perform the different operations. The Galois field linear transformer may also be compounded to perform more than one function in the operation. See the subject application at page 6, lines 12-16.

Claim 1 of the subject application recites: “An advanced encryption standard (AES) engine with real time S-box generation comprising: a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative inverse in $GF^{-1}(2^m)$ and applying an affine over $GF(2)$ transformation to obtain a subbyte transformation; and a shift register system for transforming said subbyte transformation to obtain a shift row transformation; said Galois field multiplier system being responsive in a second mode to said shift row transformation to obtain a mix column transformation and adding a round key for generating in real time an advanced encryption standard cipher function of said first data block.”

As described above, McCanny et al. clearly fails to disclose the applicants’ claimed advanced encryption standard (AES) engine with real time S-box generation that includes a Galois field multiplier system in a first mode responsive to a first data block for generating an AES selection (S-box) function by executing the multiplicative increase in $GF^1(2^m)$ and applying an


affine over GF(2) transformation to obtain a subbyte transformation. McCanny et al. also clearly fails to disclose a Galois field multiplier system that obtains both the subbyte transformation in a first mode, and obtains a mix column transformation and adds a round key in a second mode.

Thus, independent claim 1, and claims 2-31 which depend therefrom, are clearly patentable over McCanny et al. Accordingly, the applicants respectfully request that the Examiner withdraw the rejections of claims 1, 12-15 and 29 under 35 U.S.C. 102(e).

Each of the Examiner's rejections has been addressed or traversed. Accordingly, it is respectfully submitted that the application is in condition for allowance. Early and favorable action is respectfully requested.

If for any reason this Response is found to be incomplete, or if at any time it appears that a telephone conference with counsel would help advance prosecution, please telephone the undersigned or his associates, collect in Waltham, Massachusetts at (781) 890-5678.

Respectfully submitted,



David W. Poirier
Reg. No. 43,007